CLAIMS

What is claimed is:

1. A method of performing single sign-on services for a network of trusted partner sites comprising:

a) generating assertion information comprising identity information associated with a user that is authorized to sign on to said network, each of said network of trusted partner sites communicatively coupled together through a communication network;

b) generating a plurality of artifacts that are associated with said assertion information;

c) sending said plurality of artifacts to a group of trusted partner sites of said network in order to facilitate single sign-on capabilities of said network, wherein each of said artifacts allows access to said assertion information so that each of said group of trusted partner sites can individually authorize access by said user.

2. The method as described in Claim 1, wherein said a) further comprises:

a1) receiving a sign-on request from said user;

a2) retrieving said identity information associated with said user to authenticate said user; and

a3) authorizing said user access to said network when said user is authenticated.

3. The method as described in Claim 1, further comprising:

d) receiving a first artifact of said plurality of artifacts through said communication network from a first trusted partner site, said group of trusted partner sites including said first trusted partner site;

e) authenticating said first artifact to said first trusted partner site; and

f) sending said assertion information to said first trusted partner site, transparently to said user, to enable said first trusted partner site to authenticate said user and authorize access to said first trusted partner site by said user.

4. The method as described in Claim 1, further comprising:

d) receiving a first artifact of said plurality of artifacts through said communication network from a first trusted partner site not from said group of trusted partner sites, wherein said first trusted partner site received said first artifact from one of said group of trusted partner sites;

e) authenticating said first artifact; and

f) sending said assertion information to said first trusted partner site, transparently to said user, to enable said first trusted partner site to authenticate said user and

authorize access to said first trusted partner site by said user.

5. The method as described in Claim 1, further comprising:

d) receiving other assertion information from a first trusted partner site of said network of trusted partner sites, said assertion information comprising data;

e) storing said other assertion information;

f) generating another artifact associated with said other assertion information; and

g) sending said another artifact to a second trusted partner site as directed by said first trusted partner site to facilitate a transfer of said data from said first trusted partner site to said second trusted partner site, wherein said another artifact allows access to said other assertion information.

6. The method as described in Claim 1, wherein said assertion information and said plurality of artifacts substantially comply with a Security Assertions Markup Language (SAML) standard, and said network of trusted partner sites facilitates web browser single sign-on capabilities using interoperational protocols substantially complying with said SAML standard.

7. The method as described in Claim 1, wherein said a) further comprises:

sending said plurality of artifacts to a first trusted partner site of said group of trusted partner sites as directed by said user.

8. The method as described in Claim 1, wherein said a) further comprises:

sending said plurality of artifacts to a first trusted partner site of said group of trusted partner sites as directed by a second trusted partner site of said group of trusted partner site authorized access to said assertion information.

9. The method as described in Claim 1, wherein said c) further comprises:

tagging each of said plurality of artifacts for use solely by a corresponding trusted partner site in said group of trusted partner sites.

10. The method as described in Claim 1, further comprising:

d) expiring a first artifact after use of said first artifact by a trusted partner site to retrieve said assertion information.

11. A method of performing single sign-on services for a network of trusted partner sites comprising:

a) receiving a first artifact at a first trusted partner site from a central service provider, said central service provider providing single sign-on access to said network of trusted partner sites, said first artifact associated with assertion information comprising identity information associated with a user, said user desiring access to said first trusted partner site, each of said network of trusted partner sites and said central service provider communicatively coupled through a communication network;

b) sending said first artifact to said central service provider over said communication network to retrieve said assertion information;

c) receiving said assertion information from said central service provider at said first trusted partner site over said communication network; and

d) determining authorization for said user to access said first trusted partner site based on said assertion information.

12. The method as described in Claim 11, further comprising:

e) receiving a second artifact at a second trusted partner site from said central service provider, said user

desiring access to said second trusted partner site, said second artifact associated with said assertion information;

f) sending said second artifact to said central service provider over said communication network to retrieve said assertion information;

g) receiving said assertion information from said central service provider at said second trusted partner site over said communication network; and

h) determining authorization for said user to access said second trusted partner site based on said assertion information.

13. The method as described in Claim 11, wherein said central service provider previously authorizing said user to sign-on to said network of trusted partner sites, said central service provider generating and storing said assertion information.

14. The method as described in Claim 11, wherein said a) further comprises:

said receiving said first artifact at said first trusted partner site from said central service provider at a direction by a second trusted partner site authorized access to said assertion information.

15. The method as described in Claim 11, further comprising:

sending said first artifact to a second trusted partner site to facilitate access by said user to said second trusted partner site.

16. The method as described in Claim 11, wherein said assertion information and said first artifact substantially comply with a Security Assertions Markup Language (SAML) standard, and said network of trusted partner sites facilitates web browser single sign-on capabilities using interoperational protocols substantially complying with said SAML standard.

17. The method as described in Claim 11, further comprising:

e) bypassing said b) and said c) by sending said first artifact to an assertion manager controlling access to said assertion information for internal access to said assertion information when said first trusted partner site is co-located with said central service provider on a web container; and

f) receiving said assertion information from said assertion manager at said first trusted partner site.

18. A computer system comprising:

a processor; and

a computer readable memory coupled to said processor and containing program instructions that, when executed,

implement a method of performing single sign-on services for a network of trusted partner sites comprising:

a) generating assertion information comprising identity information associated with a user that is authorized to sign on to said network, each of said network of trusted partner sites communicatively coupled together through a communication network;

b) generating a plurality of artifacts that are associated with said assertion information;

c) sending said plurality of artifacts to a group of trusted partner sites of said network in order to facilitate single sign-on capabilities of said network, wherein each of said artifacts allows access to said assertion information so that each of said group of trusted partner sites can individually authorize access by said user.

19. The computer system as described in Claim 18, wherein said a) in said method further comprises:

a1) receiving a sign-on request from said user;

a2) retrieving said identity information associated with said user to authenticate said user; and

a3) authorizing said user access to said network when said user is authenticated.

20. The computer system as described in Claim 18, wherein said method further comprises:

d) receiving a first artifact of said plurality of artifacts through said communication from a first trusted partner site, said group of trusted partner sites including said first trusted partner site;

e) authenticating said first artifact to said first trusted partner site; and

f) sending said assertion information to said first trusted partner site, transparently to said user, to enable said first trusted partner site to authenticate said user and authorize access to said first trusted partner site by said user.

21. The computer system as described in Claim 18, wherein said method further comprises:

d) receiving a first artifact of said plurality of artifacts through said communication network from a first trusted partner site not from said group of trusted partner sites, wherein said first trusted partner site received said first artifact from one of said group of trusted partner sites;

e) authenticating said first artifact; and

f) sending said assertion information to said first trusted partner site, transparently to said user, to enable said first trusted partner site to authenticate said user and authorize access to said first trusted partner site by said user.

22. The computer system as described in Claim 18, wherein said method further comprises:

d) receiving other assertion information from a first trusted partner site of said network of trusted partner sites, said assertion information comprising data;

e) storing said other assertion information;

f) generating another artifact associated with said other assertion information; and

g) sending said another artifact to a second trusted partner site as directed by said first trusted partner site to facilitate a transfer of said data from said first trusted partner site to said second trusted partner site, wherein said another artifact allows access to said other assertion information.

23. The computer system as described in Claim 18, wherein said assertion information and said plurality of artifacts substantially comply with a Security Assertions Markup Language (SAML) standard, and said network of trusted partner sites facilitates web browser single sign-on capabilities using interoperational protocols substantially complying with said SAML standard.

24. The computer system as described in Claim 18, wherein said a) in said method further comprises:

sending said plurality of artifacts to a first trusted partner site of said group of trusted partner sites as directed by said user.

24. The computer system as described in Claim 18, wherein said a) in said method further comprises:

sending said plurality of artifacts to a first trusted partner site of said group of trusted partner sites as directed by a second trusted partner site of said group of trusted partner site authorized access to said assertion information.

25. The computer system as described in Claim 18, wherein said c) in said method further comprises:

tagging each of said plurality of artifacts for use solely by a corresponding trusted partner site in said group of trusted partner sites.

26. The computer system as described in Claim 18, wherein said method further comprises:

d) expiring a first artifact after use of said first artifact by a trusted partner site to retrieve said assertion information.